Supporting the Latest Standards for Post Quantum Cryptography (PQC)

In the face of growing global unrest and increasing cyber threats, the adoption of advanced security technologies is no longer optional. And, with the risk of quantum computing breaking current cryptographic systems, it is crucial to plan ahead and ensure all systems remain secure in the future.

The new FIPS 203, 204, and 205 standards recently announced by the National Institute of Standards and Technology (NIST) specify PQC algorithms in a bid to maintain the security of government systems against quantum computers. Two of the approved algorithms are based on lattice problems and the third is based on cryptographic one-way hash functions:

- **ML-KEM** is a method for distributing secret encryption keys used to encrypt and decrypt protected data.
- **ML-DSA** is an algorithm for digital signatures that allows users to prove their identity.
- **SLH-DSA** is an alternative to ML-DSA, using a hash-based algorithm.

These PQC algorithms will replace existing technology in applications that use public key cryptography today, including digital signatures for authenticating people or entities and key encapsulation mechanisms (KEMs) for establishing and managing encryption keys. Any system that incorporates PQC today will be able to provide security after the advent of a Cryptographically Relevant Quantum Computer (CRQC), whereas existing technologies (such as ECC) will become insecure.

Benefits of Using ISS Solutions

PROVEN END-TO-END SECURITY

Companies must implement proven security, including the latest algorithms, in their devices and systems. ISS solutions secure the entire device lifecycle from design and manufacturing to provisioning and updating and ongoing services for true **end-to-end security.**

MINIMIZE RISKS THROUGH SECURITY BY DESIGN

Devices are only as strong as the weakest link. They need to be designed and built with security that will last well beyond the life of the device for comprehensive protection. ISS ensures you **minimize risk** by embedding security in your offerings across the product lifecycle from birth to decommissioning.

MEET THE HIGHEST STANDARDS

Connected devices across industries need to meet stringent regulations from NIST, PCI, FDA and others. ISS helps you meet the **highest level of these standards** so you can protect against a loss of life, data, revenue and/or brand reputation.

Protecting Tomorrow’s Devices and Systems

Developers, device manufacturers and semiconductor companies need to start planning for the transition to PQC algorithms now because it takes time to propagate these changes into complex systems. The emerging technology needs to be well established before a CRQC arrives so that there is ample time for testing and rollout. Systems with data whose confidentiality needs to be protected long into the future also need to be designed using emerging security technology, because of the “store and decrypt later” risk.

In addition to the NIST activities, the National Security Agency (NSA) has announced plans to transition the security critical components of the national infrastructure to PQC and the Office of Management and Budget (OMB) has laid out a $7 billion dollar plan for making this transition across the federal government. The United States is not the only region preparing for the transition to PQC. Earlier this year the European Commission published their recommendations for making the transition, while most other major countries have given indications of their activities toward making this transition too.

INTEGRITY Security Services (ISS) recently introduced support for these PQC algorithms across its suite of embedded security, device lifecycle management (DLM), and public key infrastructure (PKI) solutions. As an industry leader, ISS has always been on top of the latest cybersecurity developments, and this development is no different. Thanks to these updates, ISS customers can leverage proven, end-to-end tools and support to create robust and secure designs for the future when quantum computing becomes pervasive.

ISS Solutions Support PQC

All ISS solutions will use PQC to maintain their security after the advent of a CRQC and our customers can count on this support in upgrading their systems.

ISS DLM PLATFORM

Quickly and confidently secure the entire device lifecycle from design and manufacturing to provision and updating with ISS DLM Platform.

ISS FLEX PRODUCTS

Easily embed the latest cryptographic functions, including PQC algorithms, into devices and systems with the ISS FLEX toolkits.

HDL IP CORES

Add high-performance security operations directly at the hardware level with crypto cores for HDL IP blocks.

The Most Experienced Provider of Embedded Security Solutions

INTEGRITY Security Services LLC (ISS) provides best-in-class embedded security products and infrastructure solutions for protecting smart connected devices from cyberattacks. With end-to-end solutions ranging from software toolkits to large-scale public key infrastructure and digital lifecycle management, ISS secures over 2 billion devices, signs and manages more than 3 billion software images per year and is trusted by some of the largest Fortune 100 companies. For more information, visit www.ghsiss.com.

© INTEGRITY Security Services, LLC. Proprietary and Confidential